

WHAT IS CLAIMED:

1. A method for securing access to passwords and personal identification numbers (PIN's) comprising the following steps:

providing a first character set from which passwords may be selected and at least one password made up of characters from said character set, and

providing a grid forming a matrix of squares totaling at least as many squares, as characters in said password.

2. The method recited in claim 1 creating a pattern made up of individual squares selected sequentially from said grid, and assigning characters from a second character set to the squares in said pattern as stand-ins for the passwords of claim 1.

3. The method recited in claim 2 wherein said password is comprised of characters in a character-based language.

4. The method recited in claim 3 wherein said character based language is English.

5. The method of claim 1 further comprising the following steps:
reducing repeated characters from said password in order to generate a unique sequence of characters to define the set of passwords, and
providing the capability to decode the reduced sequence of characters to produce a key giving access to the passwords.

6. A method for securing data and for providing secure access comprising the steps of:
creating a graphical image;
encrypting said data access using said graphical image as an encryption key, and
providing the capability to utilize said key for gaining access to said data.

BI
cm 4

7. The method recited in claim 6 wherein said encryption key is formed from a unique set of passwords selected from a character set, and utilizes a grid forming a matrix of squares.

8. The method of claim 6 further comprising
generating a randomized MasterGrid as a means for authentication,
selecting a particular MasterGrid to be associated with the encryption key, and
storing the selected MasterGrid for later access as part of the encrypted access to said data.

9. The method of claim 8 further comprising:
choosing a pathway thru said selected MasterGrid and encoding the chosen pathway as a grid reference.

10. The method of claim 9 wherein the chosen pathway is encoded as a character string corresponding to the pathway.

11. The method of claim 9 wherein the chosen pathway is encoded as a positional or sequential reference.

12. A system for securing passwords and personal identification numbers with a MasterCode having ten characters associated with ten digits, the system comprising:

means for embedding the MasterCode in a MasterGrid;
translator for translating a numeric sequence into a corresponding character sequence using the MasterCode; and
expanding said corresponding character sequence into at least one word.

13. The system as recited in claim 12 further comprising means for filling remaining entries of said MasterGrid with characters.

14. The system as recited in claim 12 wherein said MasterGrid is a rectangular grid.

15. The system as recited in claim 12 wherein said MasterGrid is a square grid.

16. The system as recited in claim 15 wherein said MasterGrid is a five by five grid.

17. The system as recited in claim 15 wherein said MasterGrid is a six by six grid.

18. The system as recited in claim 12 wherein said at least one word is a word in a character-based language.

19. The system as recited in claim 18 wherein said character based language is English.

20. The system as recited in claim 12 wherein at least seven of the ten characters are constants.

21. A device for securing passwords and personal identification numbers comprising:
a generator for creating a MasterCode having a subset of characters randomly drawn from a character set which includes numbers, symbols and alphabet characters;
means for embedding the MasterCode in a MasterGrid;
a translator for translating the MasterCode into a numeric sequence; and
assigning the numeric representations to the character sequence of passwords which may be given to the user, generated by the process or chosen by him.

22. The device as recited in claim 21 in which the MasterCode is created by generating a unique set of characters containing one instance of each character in previously assigned passwords.
23. The device as recited in claim 21 further comprising means for filling remaining entries of said MasterGrid with the characters from which the MasterCode was drawn.
24. The device as recited in claim 21 wherein MasterGrid is a rectangular grid.
25. The device as recited in claim 21 wherein said at least one password is in a character-based language.
26. The device as recited in claim 25 wherein said character based language is English.
27. A method for securing data comprising the steps of:
creating a graphical image; and
masking said data using said graphical image as key.
28. The method of claim 27 wherein said creating step includes:
forming a grid made up of rows and columns of cells;
selecting cells from said grid to form said graphical image.
29. The method of claim 27 wherein said masking step includes:
providing data that is made up typographical symbols;
using said graphical image to establish a relationship between said data and other typographical symbols; and
replacing said data with said other typographical symbols to mask said data.

30. The method of claim 29 wherein said typographical symbols are of the type selected from the group consisting of ASCII characters, upper and lower case alphabetic characters, numerical characters, and font symbols.

31. The method of claim 29 wherein said other typographical symbols are a sequence of numbers and said relationship is the ordered sequence of said data corresponding to said numerical sequence.

32. The method of claim 31 wherein the relationship of the data to the other typographical symbols includes tracing out said graphical as a pattern in sequence and placing typographical symbols from said data in cells of said grid corresponding to the graphical image.

33. The method of using a grid to gain access to encrypted passwords in which the grid is broken into cells; and wherein each cell contains a unique image, symbol or pictogram used to identify a user of subordinate device.

34. The method of claim 33 wherein the grid is linked to the user's name or other identifying input either mechanical or biocentric.

35. The method of claim 34 wherein a superior device presents an array of grids of the same size as said cell with the same content but arranged differently
and providing a selection arrangement by which a user selects one to be linked as an identifier.

36. The method of claim 34 wherein a superior device presents an array of grids of the same size as said cell with the grids content being differently and providing a selection arrangement by which a user selects one 83 to be linked as an identifier.

37. The method of claim 33 wherein a user or subordinate device creates an exclusive pattern within said grid in any cell in the grid.

38. The method of claim 35 wherein the sequence in which the cells are selected become part of the identification.

39. The method of claim 33 wherein access is obtained by first displaying an identifying grid, and gaining access only after correctly recreating a particular image, symbol or pictogram in the grid.

40. The method of claim 33 wherein access to a stored password is obtained by correctly selecting the proper identifying grid from an array of grids, and by correctly indicating the image, symbol or pictogram within the grid.

41. The method of claim 33 wherein a user chooses a particular pattern by spoken words which is stored to provide subsequent access thereto.

42. The method of claim 33 further including storage of voiceprints to insure that a proper user is reciting the words when retrieving said pattern.